Cassandra Crossing/ Il nemico nel software

(585)—Dobbiamo semplicemente abituarci a considerare "a priori" inaffidabile il software, o la questione è ancora più complessa di così?

Cassandra Crossing/ Il nemico nel software
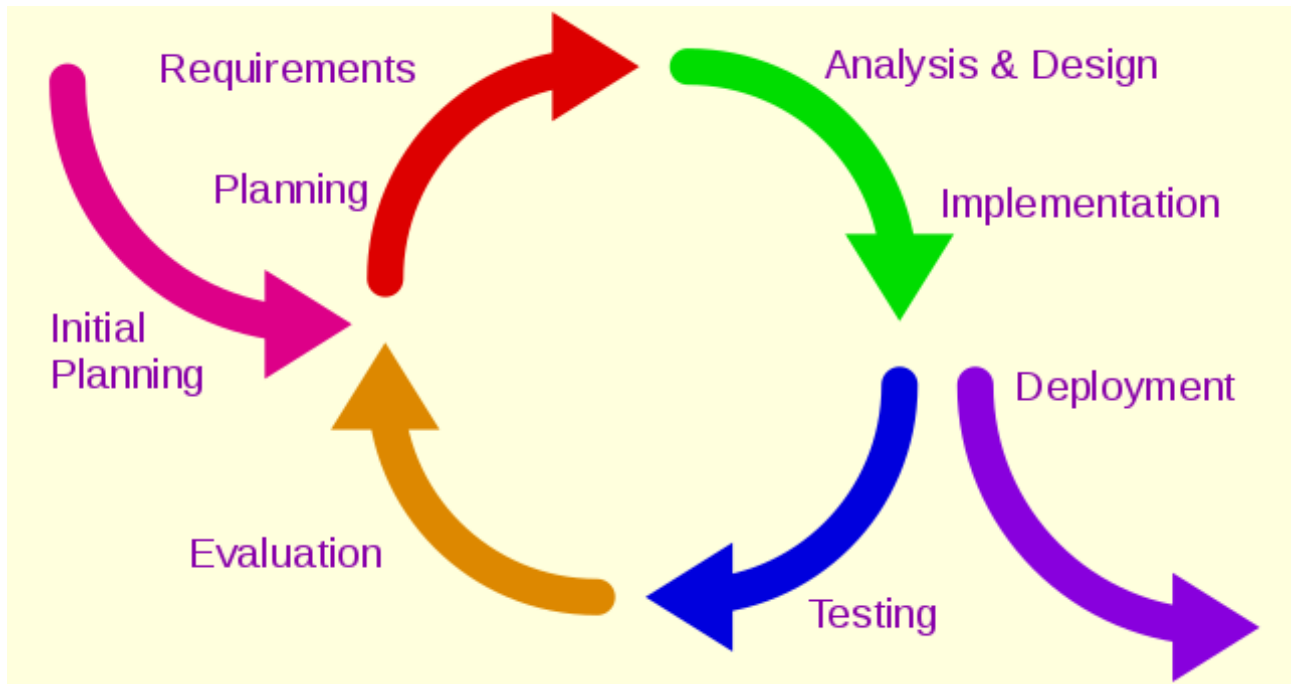
Figure 1:

(585)—Dobbiamo semplicemente abituarci a considerare "a priori" inaffidabile il software, o la questione è ancora più complessa di così?

5 giugno 2024— "*Non riesco a vedere la foresta, perché ci sono tutti quegli alberi nel mezzo*"

Con questa famosa citazione, Cassandra può riassumere la reazione tipica di chi ascolta, magari con interesse ed attenzione, le notizie che parlano di sicurezza del software, e degli sfracelli che stanno avvenendo, particolarmente riguardo agli attacchi alle catene di produzione del software.

Ed in effetti questa sintesi coglie contemporaneamente i due aspetti importanti del problema: il primo è l'affidabilità intrinseca del software, sia commerciale che libero, ed il secondo sono gli interessi di chi c'è dietro.

Cassandra non sta parlando né di facebook né delle bande che diffondono ransomware; quelli lo fanno con il consenso esplicito degli utonti, oppure grazie all'ingegneria sociale, ed ambedue non sono problemi del software.

Parliamo di conflitto, di guerra. Di fronte ad un modello di minaccia alto, il software in generale, incluso quello libero, non può dare nessuna garanzia di sicurezza o di affidabilità. Cassandra ve ne ha già dato la dimostrazione.

Questo è dovuto alle modalità con cui il software viene prodotto e distribuito o commercializzato. Nessuna di esse è pensata in termini di affidabilità o di sicurezza, ma solo di convenienza, virtuosa o viziosa che sia.

Nel caso del software commerciale, come sanno tutti quelli che ci hanno lavorato, esso viene venduto appena funzionante, e si recepiscono poi in parte le segnalazioni dei clienti/betatester, secondo la comodità e la convenienza del produttore, il quale nel frattempo si difende dai rischi economici con polizze assicurative e stuoli di lobbisti ed help desk.

Nel caso del software libero, nemmeno uno scrutinio completo dei sorgenti, impresa titanica se estesa a tutto l'ambiente di esecuzione del software stesso, può dare garanzie assolute, considerato il livello di sofisticazione dimostrato da chi di mestiere produce software malevoli, o compie azioni ostili con tecnologie informatiche.

Il software libero, ed anche quello open source, invece vivono nel perenne bazar, già teorizzato nello scorso millennio, e non si potranno mai schiodare da lì. Sarà software mediamente scritto bene e con attenzione, ma non potrà mai essere affidabile contro attaccanti di alto profilo.

Riassumendo di nuovo in maniera più "tecnica":

- [il software attualmente in uso ed i relativi modelli di sviluppo, sia commerciale che aperto, non sono né affidabili, né emendabili per poterlo diventare.]
- [Quindi, per impieghi ad alto rischio, oppure per impieghi in ambito di conflitto asimmetrico, non esisterà mai nessun "software affidabile", nessuna difesa "a priori". Le guerre asimmetriche saranno guerre di trincea, dove vince chi fa più morti.]
- [La convivenza con grandi rischi dovuti al software è inevitabile ed ineliminabile, come quella con la Bomba o con i cosiddetti "disastri industriali".]
- [Una mitigazione, e non una soluzione, potrà venire solo da diplomazia, trattati ed alleanze.]

Certamente, la tecnologia non potrà mai offrirci una soluzione.

Viviamo già oggi con software inaffidabile, ed utilizzabile da "altri" come arma, e ci dovremo convivere anche nel futuro prevedibile. Ve lo garantisce la vostra profetessa preferita.

Non ci resta che il duro lavoro di farcene tutti una ragione.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

***Licenza d'utilizzo**: i contenuti di questo articolo, dove non diversamente indicato, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link.

By Marco A. L. Calamari on June 5, 2024.

Canonical link

Exported from Medium on August 27, 2025.